ProtectDrive

User Manual

Revision: B00

eracom TECHNOLOGIES

THIS PAGE INTENTIONALLY LEFT BLANK

Preface

Copyright

All intellectual property is copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of:

Eracom Technologies
28 Greg Chappell Drive
Burleigh Heads, Queensland 4220
AUSTRALIA

	National	International
Voice:	(07) 5593 4911	+ 61 7 5593 4911
Fax:	(07) 5593 4388	+ 61 7 5593 4388

Website: www.eracom-tech.com

Copyright © Eracom Technologies.
All rights reserved.

Disclaimer

Eracom makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Eracom reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Eracom to notify any person or organization of any such revisions or changes.

Publication Improvements

Eracom invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be dispatched to the above address.

Technical Support

If you encounter a problem while operating this product, please make sure that you have read the documentation.

If you cannot resolve the issue, please contact your ProtectDrive System Administrator.

Revision History

Revision	Release Date	Description
A0	June 2002	Initial Release
A1	September 2, 2002	Rev 1.0
A2	September 18, 2002	Rev 1.1
A3	December 13, 2002	Remote Password Recovery.
A4	July 2003	New features for 6.0.0 release
A5	July 22, 2003	Print anomaly corrections
A6	August 29, 2003	Add auto-logon functionality
A7	September 17, 2003	Add token authentication and new 6.1.0 features
A8	December 17, 2003	Addition of 3DES and NT support
A9	January 7, 2004	Removed Upgrade support for 6.1.0
A10	March 2004	Updated to meet requirements of CC Evaluation and PD V7.0.2
A11	June 2004	Separate revision for CC evaluation of ProtectDrive 7.0.2
A12	June 2004	Updated for ProtectDrive 7.1.0
A13	October 2004	Separate revision for CC evaluation of ProtectDrive 7.0.3 derived from Rev A11 Updated version information to V7.0.3 Reformatted Pages, TOC, Header and Footer
A14	January 10, 2005	Derived from revision A12 Updates for ProtectDrive 7.2.0 Updates to screen shots Ability to boot from floppy after Preboot logon removed Details regarding defragmentation removed
B00	February 22, 2005	A14 User Manual was restructured into ProtectDrive Administration Guide (Rev A00) and ProtectDrive User Manual (Rev B00). The B00 contains PD 7.3 functionality.

THIS PAGE INTENTIONALLY LEFT BLANK

 © Eracom Technologies

Table of Contents

Preface ..... **i**
Technical Support ii
Chapter 1 Introduction **1**
Product Overview 1
Who should read this document? 3
Chapter 2 Logging On to Your ProtectDrive Secured PC **5**
Logging On with Smartcard/Token and PIN 6
Logging On with Username/Password/Domain Name 7
What to Do If Your Preboot Log On Fails 8
Incorrect Preboot Username and/or Password *8*
Preboot Log On Failure Due to System Inoperability *8*
Chapter 3 Logging On to Windows **9**
Manual Windows Log On 9
Logging On to Windows with Smartcard/Token and PIN *9*
Logging On to Windows with Username/Password/Domain Name *10*
Chapter 4 Using Windows with ProtectDrive **13**
ProtectDrive User Authentication Activity Tracking 13
Disk Encryption Warning 14
ProtectDrive System Tray Icon 14
Using Windows Folder Compression Application on Your ProtectDrive Secured PC 15
Using Windows System Restore Utility on Your ProtectDrive Secured PC 15
Changing Your ProtectDrive Preboot Password 16
Invalid ProtectDrive Password Format Error *17*
Disallowed Floppy Device Access Error 18
Disallowed COM/LPT Port Access Error 18
Chapter 5 Encrypting Hard Drives **19**
Local Machine Configuration Utility 19
Specifying the Encryption Algorithm *22*
Disk Encryption Example 23
Chapter 6 Troubleshooting **27**
What to Do If You Misplace Your Smartcard/Token or Forget Your PIN 27
What to Do If You Forget Your Password 28
What to Do If You Do Not Have a Preboot User Account 29
New User Preboot Introduction Procedure *30*

THIS PAGE INTENTIONALLY LEFT BLANK

© Eracom Technologies

Chapter 1
Introduction

Product Overview

In today's computing environment hard drives (HDD) have become mass repositories of proprietary information. The widely used Windows operating systems provide adequate data privacy whether on a stand-alone machine or a networked computer (in most operating environments). However, insufficient data security protection exists in a case of system (or HDD) loss due to malicious intent. Unless appropriate data protection measures are taken, any HDD can be removed from the system, and data on it may be read. Furthermore, the system can be accessed via its Floppy Drive(s), Serial (COM) and/or Parallel (LPT) ports. To fill these data security gaps Eracom has developed the ProtectDrive computer system security application.

One of the PC security functions provided by ProtectDrive is *User Authentication* (log-in) into the system. This is a two-stage sequential process as follows:

Preboot Authentication — The user is required to provide valid log-in credentials right after the computer is turned on and *before* Windows loads.

Windows Authentication — This is the actual Windows log-in based on the user's Windows authentication methods in existence prior to the ProtectDrive installation. Generally ProtectDrive will be configured by the System Administrator to perform the Windows log-in *automatically* requiring no user input. In isolated cases, however, the user may be required to log into Windows separately following their ProtectDrive (Preboot) log-in.

The above two methods of user authentication typically rely on the user's existing Windows log-in credentials, which are configured by the System Administrator and come in two distinct flavors:

Smartcard or Electronic Token and PIN	The user inserts a Smartcard into a reader and then types in their PIN. Alternatively, the user may insert a Token into the USB port and then type in their PIN.
Username, Password, Domain Name	The user types in their Windows username, password, and domain name.

Users will need to contact their ProtectDrive System Administrator for detailed instructions on how to log-in to their respective systems.

© Eracom Technologies

Who should read this document?

This document is intended for computer end-users who use their PC systems for every day operations such as word processing, e-mail, Internet access, etc. The scope of this document assumes that your computer is managed by an IT professional. Typically this would be your *System Administrator*. This person is generally resposibile for configuration and maintenance of various computer system components such as ProtectDrive.

This document introduces ProtectDrive operation from the end-user point of view and covers the following ProtectDrive operational issues:

- How to turn on and log on to your ProtectDrive secured PC
- How to log on to Windows on your ProtectDrive secured PC
- What to do if you misplace your Smartcard/Token or forgot your PIN
- What to do if you forget your Password
- What to do if your log on fails
- How to use Windows with ProtectDrive
- How to perform Hard Drive Encryption

Minimal technical knowledge is required to digest this material. Please consult your *System Administrator* as well as the the latest version of the *Protect Drive Administration Guide* for issues pertaining to ProtectDrive installation, data encryption, system and user managmeent; and disaster recovery.

THIS PAGE INTENTIONALLY LEFT BLANK

© Eracom Technologies

Chapter 2
Logging On to Your ProtectDrive Secured PC

Once the user presses the power button on their ProtectDrive secured PC, it will turn-on and boot normally. The user is then presented with one of the *Preboot Log On Screens* shown in Figures 1 and 2.

The *Smartcard/Token/PIN* users will use the screen shown in Figure 1, while the *Username/Password/Domain Name* users will use the one in Figure 2.

The user may display **Help** in both of these screens by pressing the **[F1]** function key.

Please note that if the system has been configured by the System Administrator to allow Smartcard/Token/PIN access as well as Username/Password/Domain Name; then the user you may toggle between these two screens by using the **[F2]** function key.

Logging On with Smartcard/Token and PIN

The Smartcard/Token/PIN users use the Preboot authentication screen shown in Figure 1. This screen displays immediately after the system has been turned on. Logging on in this case is a two step process:

1. The user inserts their Smartcard or Token into the reader.
2. The user types their PIN into the screen shown in Figure 1 below.

Following the above procedure the system will proceed to loading Windows. In most common ProtectDrive configuration scenarios the system will log the user into Windows *automatically*. However, in isolated instances the System Administrator may configure ProtectDrive to require user to log on to Windows manually. Please refer to Chapter 3 – Logging On to Windows.

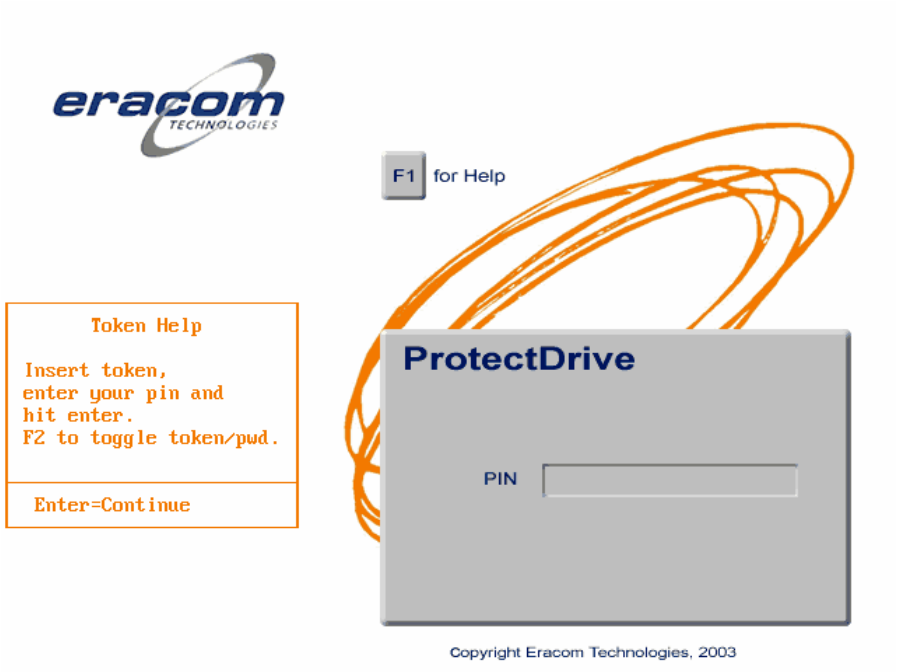


Figure 1 – Smartcard/Token PIN Preboot Log On screen

© Eracom Technologies

Logging On with Username/Password/Domain Name

The Username/Password/Domain Name users use the Preboot authentication screen shown in Figure 2. This screen displays immediately after the system has been turned on. Logging on in this case is a four step process:

1. Type in your Username
2. Type in your Password
3. Selects the relevant Windows Domain by using **[UP-ARROW]** and **[DOWN-ARROW]** keys in the **Domain** field.
4. Press **[ENTER]**

Following the above procedure the system will proceed to loading Windows. In most common ProtectDrive configuration scenarios the system will log the user into Windows *automatically*. However, in isolated instances the System Administrator may configure ProtectDrive to require user to log in to Windows separately. Please refer to Chapter 3 – Logging On to Windows.

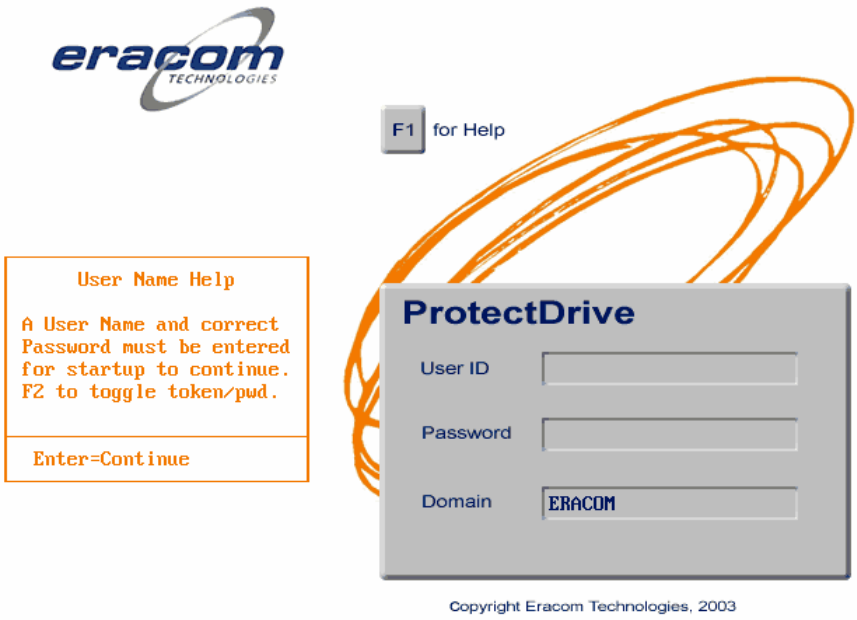
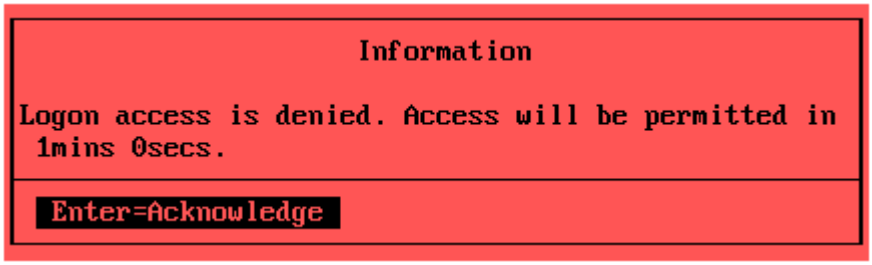


Figure 2 – Username/Password/Domain Name Preboot Log On Screen (Domain=PDHOST2 is just an example)

What to Do If Your Preboot Log On Fails

Incorrect Preboot Username and/or Password

If the user fails to provide ProtectDrive with a correct Preboot Username and/or Password three (3) consecutive times (this value may differ on some systems as it is at System Administrator's discretion), ProtectDrive will display the following *User Lock Out Screen.* A three (3) minute count down period will commence (this value is also at the System Administrator's discretion). The system will be inoperable during this time. Please contact your System Administrator for further assistance.



Preboot Log On Failure Due to System Inoperability

If any of the ProtectDrive system files and/or encrypted hard drive partitions experience corruption, the user may not be able to authenticate into the system at Preboot. In these isolated instances an error screen similar to the one shown below will display. The screen will list an *ACS Error Number*, which the user needs to communicate to the System Administrator. Please note that ACS0301 is just an example.

© Eracom Technologies

Chapter 3
Logging On to Windows

Typically the ProtectDrive system will be configured by the System Administrator to *automatically* log the user into Windows following their successful Preboot authentication. In this case no further user input is required, and Windows will load normally. Please proceed to Chapter 4 – Using Windows on Your ProtectDrive Secured PC.

Manual Windows Log On

If the System Administrator has setup the system to require users to manually log on to Windows; then one of the two Windows Welcome Screens shown in Figures 3 and 4 will display immediately following user's successful Preboot authentication. The *Smartcard/Token/PIN* users will use the screen shown in Figure 3 while the *Username/Password/Domain Name* users will use the one in Figure 4.

Logging On to Windows with Smartcard/Token and PIN

The Smartcard/Token/PIN users use the Windows Welcome Screen shown in Figure 3 below.

Figure 3 – Smartcard/Token/PIN Windows Welcome Screen

The following two step procedure is used to manually log in to Windows:

Insert your Smartcard or Token into the reader

The following Windows Log On Screen displays:

Enter your PIN

Windows will proceed to load normally and you will see your familiar Windows Desktop appear. Refer to Chapter 4 – Using Windows on Your ProtectDrive Secured PC.

Logging On to Windows with Username/Password/Domain Name

The Username/Password/Domain Name users will use the Windows Welcome screen shown in Figure 4 below.

Figure 4 – Username/Password/Domain Name Windows Welcome Screen

© Eracom Technologies

The following procedure is used to manually log in to Windows:

Press **CTRL-ALT-DEL** in the Windows Welcome Screen shown in Figure 4.

The following Windows Log On Screen displays:

Enter your Windows Username and Password supplied by your system Administrator

Select your Windows Domain by using **[UP-ARROW]** and **[DOWN-ARROW]** keys

Press OK

Windows will load normally and you will be presented with your Windows Desktop. Please proceed to Chapter 4 – Using Windows on Your ProtectDrive Secured PC.

THIS PAGE INTENTIONALLY LEFT BLANK

© Eracom Technologies

Chapter 4
Using Windows with ProtectDrive

ProtectDrive is designed to run with minimal visibility to the end user. The intent is to produce no effect on normal computer system operation. However, some minor software compatibility issues pertaining to various MS Windows programs and utilities exist and need to be taken into consideration. The following chapter outlines various MS Windows and software compatibility related considerations the user needs to make when operating a computer system secured by ProtectDrive.

ProtectDrive User Authentication Activity Tracking

The System Administrator may configure your system to inform you of your ProtectDrive authentication activity. If this is the case, then after successful Windows authentication and right before the loading of the Windows Explorer Shell the following two (2) ProtectDrive information dialogs will display alerting the user to all of their ProtectDrive Preboot authentication activity to date.

ProtectDrive Information
Current User : Administrator
Domain: ERACOM
Last logon : Tuesday, March 15, 2005 09:54:53
Password last changed : (never)
Logons since last password change : 5
Total logons : 5
OK

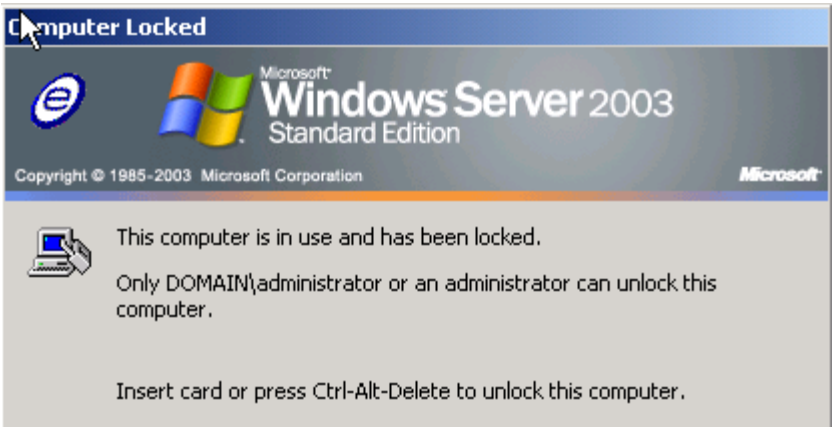
ProtectDrive Warning
Since your last logon there has been :
3 unsuccessful logon attempt(s) with your user name
Since the last system logon there has been :
3 unsuccessful logon attempt(s)
The last unsuccessful logon attempt was made on Tuesday, March 15, 2005 09:56:02.
OK

Disk Encryption Warning

If the system has been configured by the System Administrator to alert users of incomplete encryption status of any of the hard disk partitions, and any of the drives are found to be unencrypted; then the following warning message will display immediately after the loading of the Windows Explorer Shell.

ProtectDrive System Tray Icon

On all ProtectDrive secured PCs a Windows System Tray icon ( ) located in the right lower corner of the Desktop will appear indicating that this PC is protected. **DOUBLE-CLICK** on this icon to lock the Windows Desktop. This will result in the Windows screen similar to the following. Press **CTRL-ALT-DEL** to log back into the Windows Desktop.


Computer Locked
Microsoft
Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
This computer is in use and has been locked.
Only DOMAIN\administrator or an administrator can unlock this computer.
Insert card or press Ctrl-Alt-Delete to unlock this computer.

© Eracom Technologies

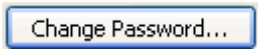
Using Windows Folder Compression Application on Your ProtectDrive Secured PC

Windows folder compression is fully supported with one exception. The ProtectDrive system files directory (**C:\SECURDSK**) is write-protected and must not be removed or compressed. Compressing this directory will interfere with the normal operation of ProtectDrive.

Using Windows System Restore Utility on Your ProtectDrive Secured PC

Windows System Restore points created prior to the ProtectDrive install are rendered useless. System can only be restored to any restore point created following the ProtectDrive install.

Changing Your ProtectDrive Preboot Password

Press **CTRL-ALT-DEL** and select 

Select the appropriate domain in the **Log on to** field and specify the new password.

For local Windows (see **"this computer"** above) the new password change becomes effective immediately.

For Windows Domain (below) the user will need to log out of Windows and log back in. This will propagate the new password to the ProtectDrive Preboot User dB. If the user does not follow this procedure, they would have to use their old password at preboot. Once they log into Windows Domain with their new password, this new password will propagate to the ProtectDrive Preboot User dB.

Invalid ProtectDrive Password Format Error

If in the process of changing their Windows (Domain) Password the user enters a password which does not satisfy the password strength requirements imposed by the System Administrator the following error will display. The user needs to either try a different password or contact their System Administrator for further assistance on selecting an appropriate password.

ProtectDrive Error
Invalid ProtectDrive password.
Your password must be between 8 and 20 characters long, must not be the same as your Username, cannot contain more than 2 repeated characters, and cannot be the same as any of the last 7 passwords you have used.
OK

Please note that in the above screen the minimum password length of 8 characters is just an example. This value may differ on your system at the System Administrator's discretion.

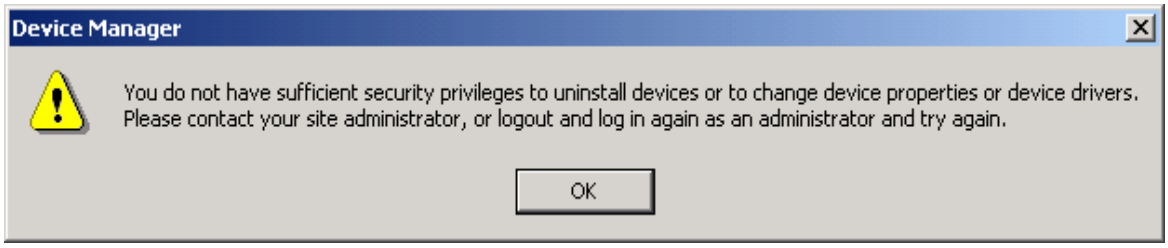
Disallowed Floppy Device Access Error

ProtectDrive Administrator may configure the system to disallow user access to the floppy drive(s) as well as the COM and LPT ports. If a user who's *Device Access Permissions* are disabled attempts to access the floppy drive the following dialog will display.

In these instances the user is advised to contact their respective system administrator for further assistance.

Disallowed COM/LPT Port Access Error

If a user who's ProtectDrive *Device Access Permissions* are disabled attempts to access any of the devices including the COM and LPT ports the an error will occur. This error may be displayed by the actual software application the user is running, through which the device is being accessed. For example while using the Windows HyperTerminal the user may try to use the COM port(s) permissions for which are currently disabled by ProtectDrive. In this case HyperTerminal will display some sort of device access (or read/write) error. In isolated instances ProtectDrive itself will display the following message. In these instances the user is advised to contact their respective system administrator for further assistance.

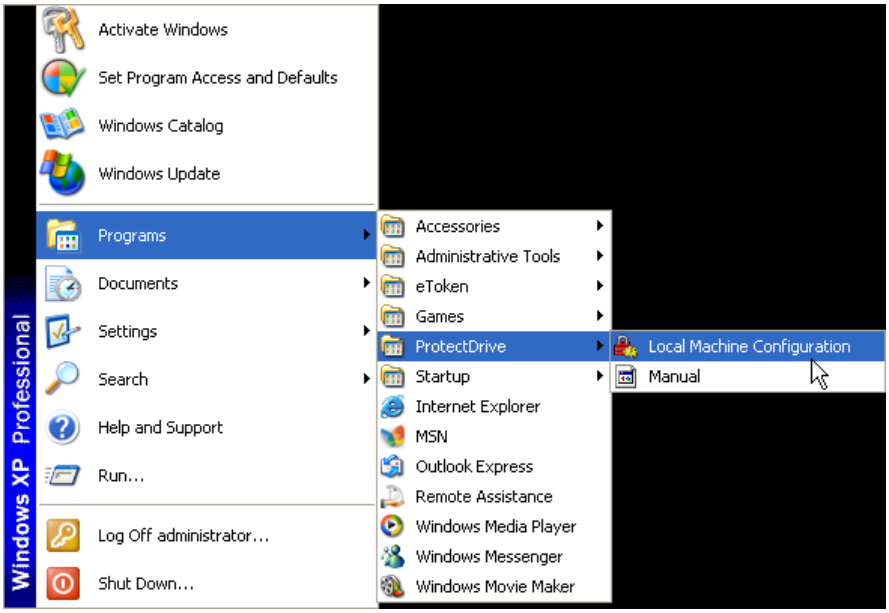

Device Manager
You do not have sufficient security privileges to uninstall devices or to change device properties or device drivers.
Please contact your site administrator, or logout and log in again as an administrator and try again.
OK

© Eracom Technologies

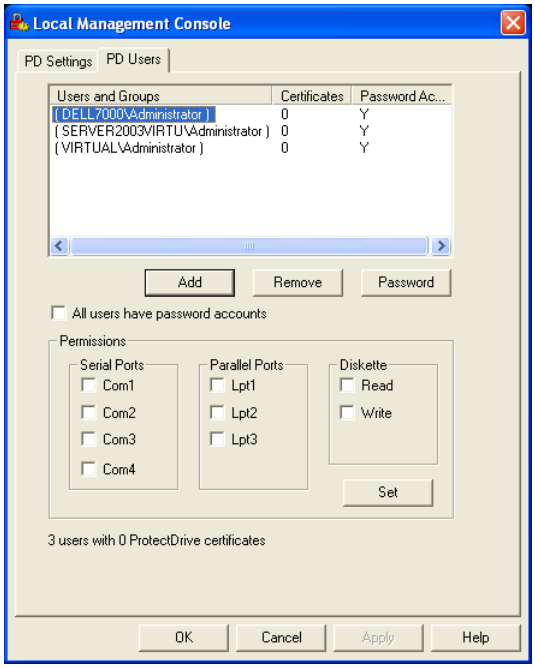
Chapter 5
Encrypting Hard Drives

Please note that in the current release of ProtectDrive the Local Machine Configuration Utility is **read-only**. Configuration data in the **PD Settings** and **PD Users** tabs can be viewed locally, but **not** modified at this time.

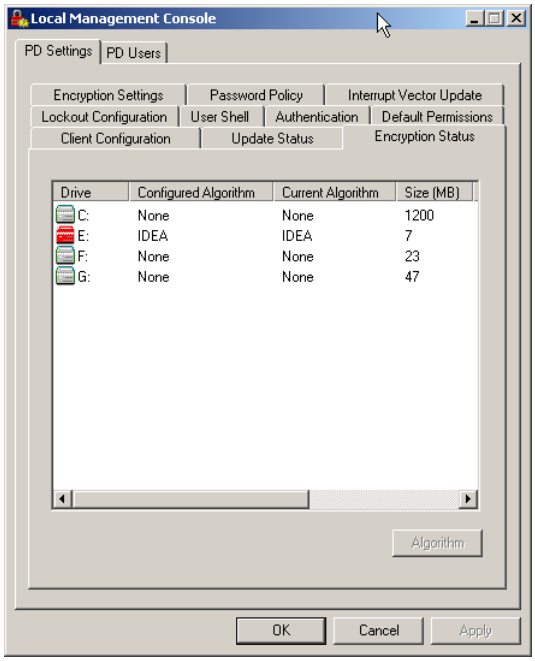
Local Machine Configuration Utility

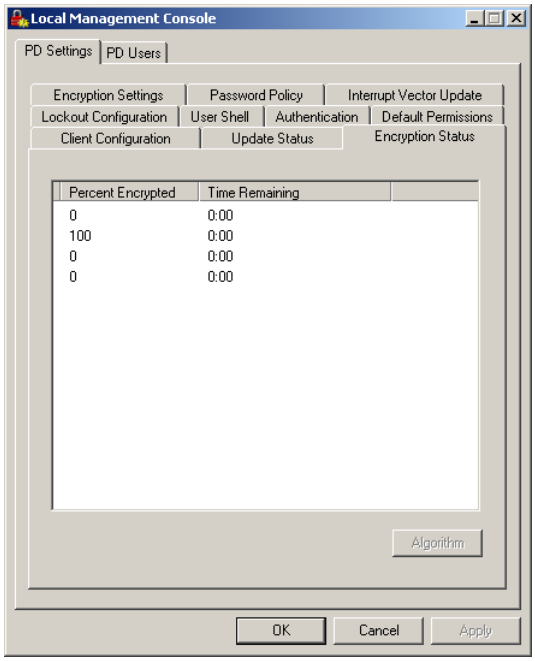


The **PD Users Tab** lists all the users currently in the Preboot User dB. Each user's device access **Permissions** is also shown here.



The **Encryption Status Tab** located under the **PD Settings Tab** allows for local hard drive encryption.



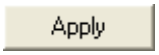
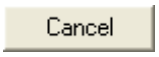


© Eracom Technologies

The displayed columns are as follows:

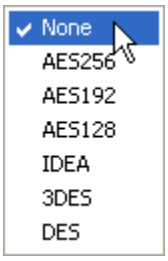
Drive	Partition drive letter
Configured Algorithm	Algorithm selected for encryption of the given partition
Current Algorithm	All encrypted partitions will display the algorithm used for their encryption.
Size (MB)	The size of the partition
Percent Encrypted	Status indicator during on-going encryption operation
Time Remaining	Status indicator during on-going encryption operation

Buttons on this dialog are as follows

	Displays Encryption Algorithm selection dialog
	Starts the encryption process. If the System Administrator configured ProtectDrive to disallow disk encryption, this button will be disabled.
	Cancels/Pauses the encryption process for all partitions where encryption has not yet commenced. If the encryption process already started on a given partition pressing this button will pause the encryption process.
	Starts the encryption process and closes the Local Machine Configuration utility. If the System Administrator configured ProtectDrive to disallow disk encryption; this button will be disabled.

Specifying the Encryption Algorithm

Press Algorithm then select the encryption algorithm from the following dialog. Note that algorithm list shown below may very based on your system configuration.



Please consult with you System Administrator for guidance on which Encryption Algorithm best suits your system.

None Selecting this will cause an encrypted drive to be decrypted. Please note that this setting is disabled for users without administrative privilege. Hard drive decryption is only allowed for System Administrators

DES The DES cipher is a publicly tested 56-bit key 64-bit block cipher. ProtectDrive operates this cipher in CBC Mode. Details on the cipher are publicly available from many sources.

3DES The Triple DES cipher is a publicly tested 112 bit key 64 bit block cipher. ProtectDrive operates this cipher in CBC mode. Details on the cipher are publicly available from many sources.

IDEA The International Data Encryption Algorithm (IDEA) was developed in the early 1990s. It operates using 64-bit blocks and 128-bit keys. ProtectDrive uses the cipher in CBC mode.

AES128
AES192
AES256

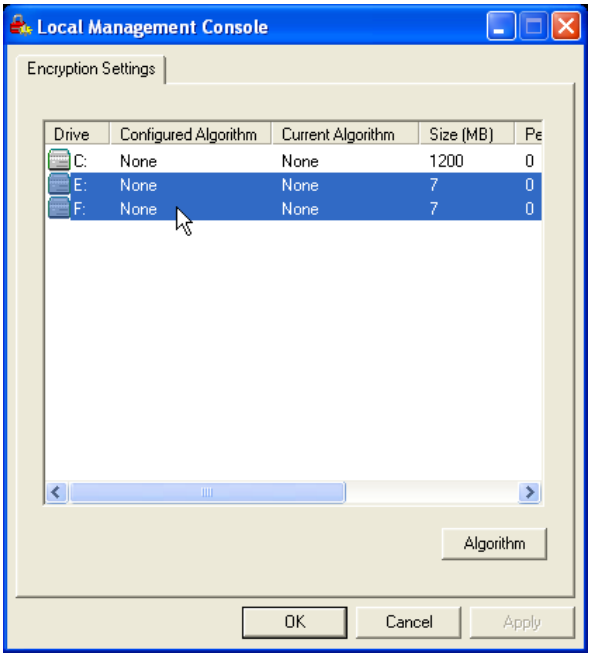
The Advanced Encryption Standard was announced by NIST in November 2001 in FIPS PUB 197. It is symmetric block cipher that processes 128-bit data blocks and uses 128-bit, 192-bit or 256-bit keys. ProtectDrive uses the cipher in CBC mode.

© Eracom Technologies

Disk Encryption Example

In the following example drive partitions **E** and **F** will be encrypted using the IDEA algorithm. Then drive **E** will be re-encrypted using the AES192 algorithm.

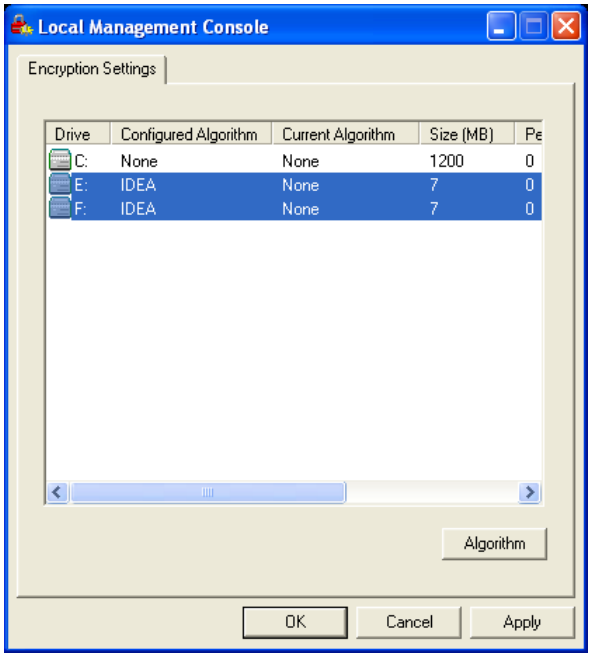
Using the **`CTRL-Mouse-Click`** or **`SHIFT-Mouse-Click`** allows for selection of multiple disks for encryption.



Press

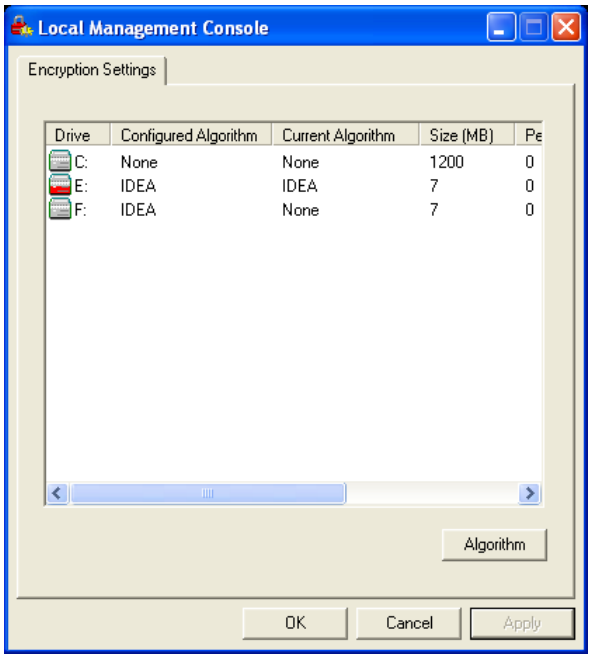
Select IDEA

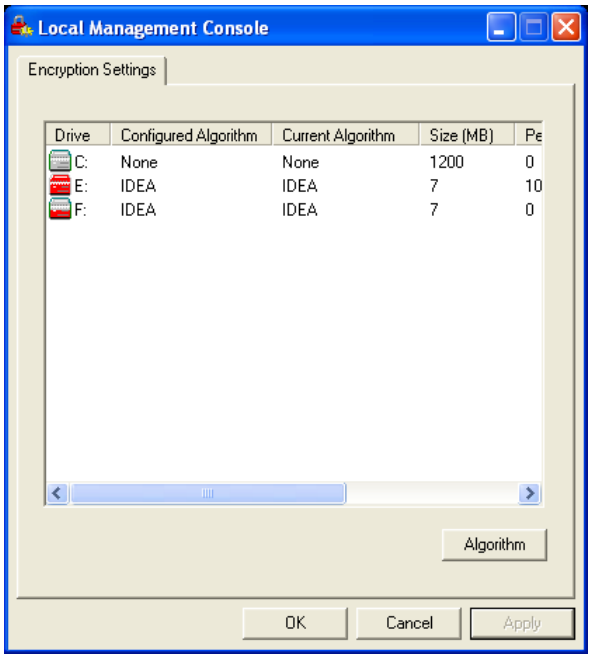
Drives **E** and **F** are configured to be encrypted



Press Apply and encryption will commence shortly

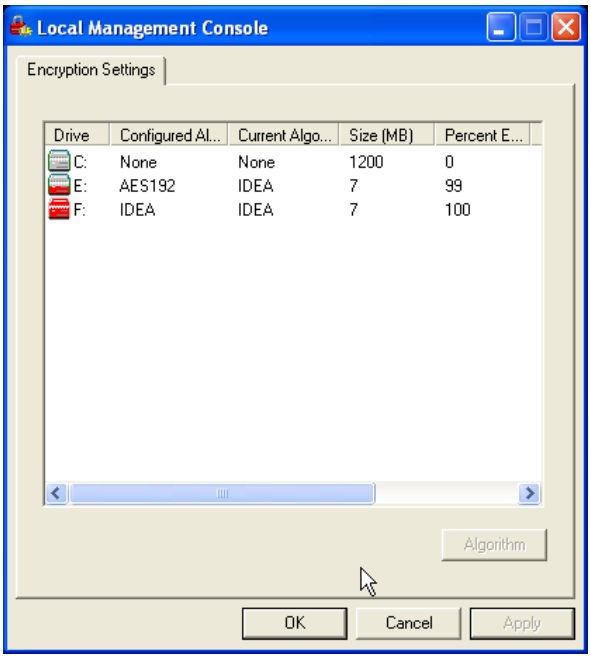
The following will display as encryption progresses on drive E and then F





© Eracom Technologies

Once the encryption completes on drives **E** and **F** you may re-encrypt drive **E** (for example) to a different algorithm. Select drive **E** and then click Algorithm to select an alternative algorithm. Press Apply and drive **E** will be re-encrypted with the newly selected algorithm.



THIS PAGE INTENTIONALLY LEFT BLANK

© Eracom Technologies

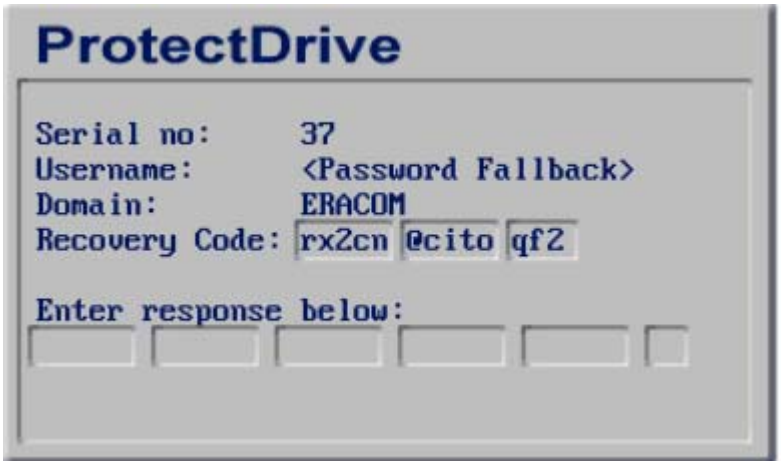
Chapter 6
Troubleshooting

What to Do If You Misplace Your Smartcard/Token or Forget Your PIN

If a *Smartcard/Token/PIN* user misplaces their Smartcard/Token or forgets their PIN, access to the system may be achieved by exercising the ProtectDrive *Preboot Password Fallback Procedure* as follows:

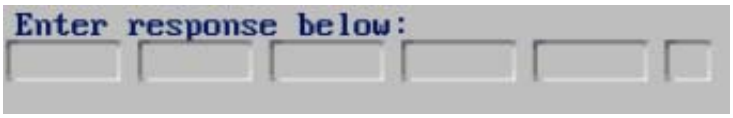
Press **SHIFT-F9** while the cursor is placed into the **"PIN"** field of the Smartcard/Token/PIN Preboot Log On Screen shown above.

The ProtectDrive Password Fallback Challenge/Response Screen displays.



Contact your System Administrator (either in person or by phone) and communicate to them the displayed *Recovery Code (Challenge)*. Please note the code shown below is just an example.

In return the Administrator will communicate to you to the *Response Code*. Enter this code into the **"Enter response below:"** field shown below.



At this point Windows will proceed to load normally and will either log you on *automatically* or *manually* depending on how the System Administrator configured ProtectDrive. For manual Windows log on please review Chapter 3 – Logging On to Windows.

What to Do If You Forget Your Password

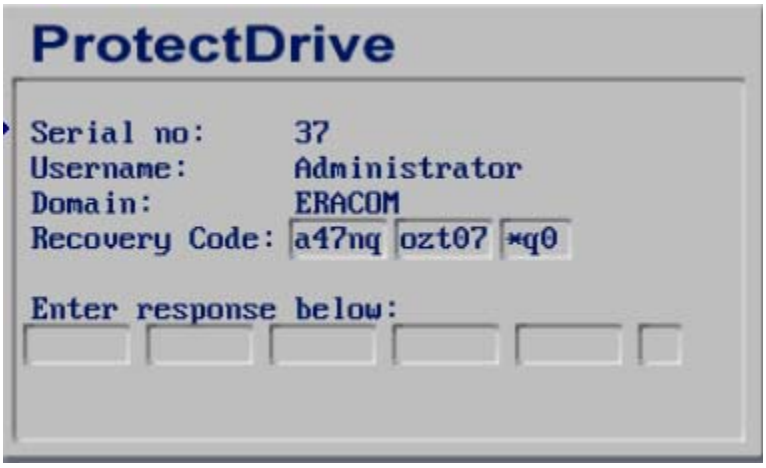
If a *Username/Password/Domain Name* user forgets their Password, the *Preboot Password Recovery Procedure* can be used to gain access to the system as follows:

Enter your Username into the **"User ID"** field of the Username/Password/Domain Name Log On Screen shown above.

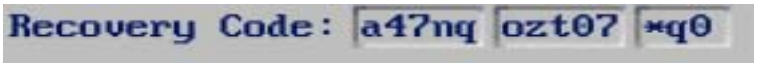
Next place the cursor into the **"Password"** field and press **SHIFT-F10**

The Password Recovery Challenge/Response Screen displays.

© Eracom Technologies



Contact your System Administrator (either in person or on the phone) and communicate to them the displayed *Recovery Code* (*Challenge*) along with your *Username*. Please note the code displayed below is just an example.



The Administrator in turn will communicate to you the appropriate *Response Code*. Enter the *Response Code* into the **`Enter response below:`** field.

At this point Windows will proceed to load normally and will either log you on *automatically* or *manually* depending on how the System Administrator configured ProtectDrive. For manual Windows log on please review Chapter 3 – Logging On to Windows.

What to Do If You Do Not Have a Preboot User Account

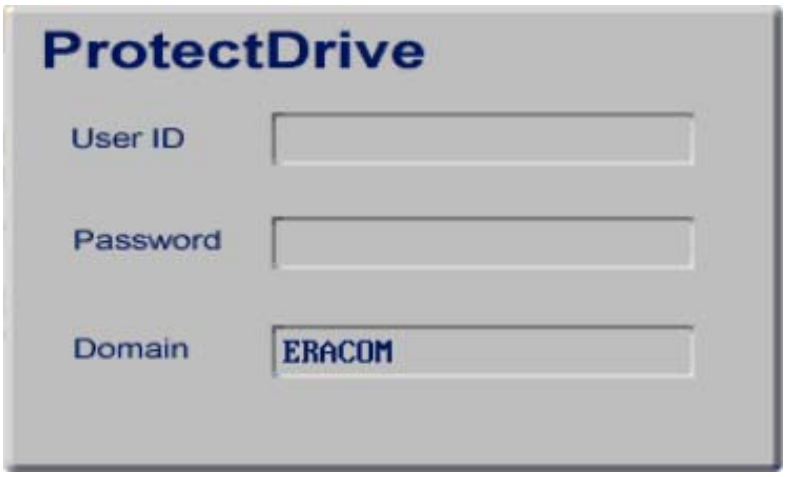
Username/Password/Domain Name users who have not yet had the opportunity to log on to their ProtectDrive secured PC may be required by their System Administrator to execute the following *New User Introduction Procedure* during their first-time-ever system log on.

Please note that this procedure applies only to the *Username/Password/Domain Name* authentication method. New *Smartcard/Token/PIN* users have new Preboot accounts created for them by the System Administrator and, therefore, are able to log-in to the system without undergoing any additional procedures such as the one described in this section.

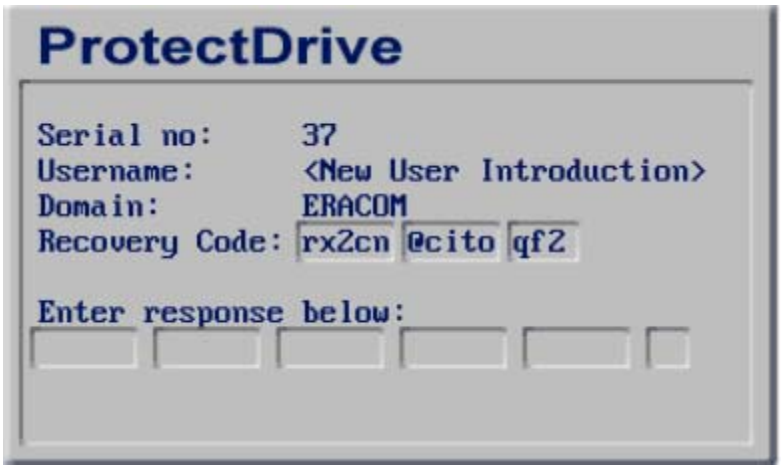
New User Preboot Introduction Procedure

Place the cursor into the **"User ID"** filed of the Username/Password/Domain Name Log On Screen (below). Note: ERACOM domain is just an example.

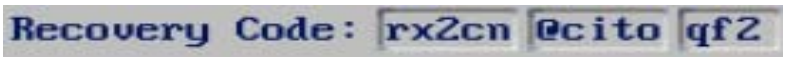
Press **SHIFT-F9** function key while the cursor is placed into the **"User ID"** field



The New User Introduction Challenge/Response Screen displays.



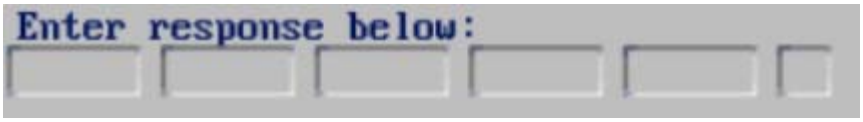
Contact your System Administrator (either in person or phone) and communicate to them the displayed *Recovery Code (Challenge).* Note: the code listed below is just an example.



In turn the System Administrator will communicate to you the appropriate *Response Code*.

© Eracom Technologies

Enter the *Response Code* into the **`Enter response below:`** field and one-time-only Preboot access to the system is granted. The user then proceeds to normal Windows log-in. The user's next system log-in will be as described in Chapter 2 - Logging On to Your ProtectDrive Secured PC.



END OF DOCUMENT

© Eracom Technologies